



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/542,904

07/20/2005

Johan Paul Marie Gerard Linnartz

NL 030088

1783

24737

7590

04/30/2008

PHILIPS INTELLECTUAL PROPERTY & STANDARDS

P.O. BOX 3001

BRIARCLIFF MANOR, NY 10510

EXAMINER

CHAI, LONGBIT

ART UNIT

PAPER NUMBER

2131

MAIL DATE

DELIVERY MODE

04/30/2008

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/542,904	Applicant(s) LINNARTZ, JOHAN PAUL MARIE GERARD	
	Examiner Longbit Chai	Art Unit 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 20 July 2005.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-10 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-10 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 20 July 2005 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date <u>2/23/2007</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Priority

1. Applicant's claim for benefit of foreign priority under 35 U.S.C. 119 (a) – (d) is acknowledged.

The application is filed on 7/20/2005 but is a 371 case of PCT/IB03/03622 application filed 12/24/2004 and has a foreign priority application filed on 1/24/2003.

Claim Objections

2. Claim 9 is objected to because of the following informalities: “A playback and/or recording apparatus (400) comprising a device (101) as claimed in claim 8 ” should be “The device of claim 8, comprising a playback and/or recording apparatus”. Appropriate correction is required.

3. Regarding claim 1, 3, 8 and 9, the drawing numbers, such as “a storage medium (101)” as recited in the instant claim, are suggested to be removed to minimize the dependency between the claims and the drawings so that any number changed in the drawing would not mutually impact the other number used in the claims.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Art Unit: 2131

4. Claim 10 is rejected under 35 U.S.C. 101 because these claims are directed to “A computer program product”, which is merely an example of functional descriptive material, (i.e. software, per se), and is nonstatutory under 35 USC 101. By not limiting the computer program product to being stored on a computer readable storage medium, there is a lack of the required functional and structural interrelationship between the software and the computer storage medium that permits the functionality of the software to be realized upon access by a processor. This ability is what underlies the ability to provide a practical application. Warmerdam, 33 F.3d at 1361, 31 USPQ2d at 1760. In re Sarkar, 588 F.2d 1330, 1333, 200 USPQ 132, 137 (CCPA 1978). See MPEP § 2106 (IV.B).1(a).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

A person shall be entitled to a patent unless –

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 1, 2, 3 and 7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Linnartz (U.S. Patent 6,209,092), in view of Lotspiech et al. (U.S. Patent 6,888,944).

As per claim 1, Linnartz teaches a method of granting access to content on a storage medium, comprising:

obtaining cryptographic data (Y) from a property of the storage medium (Linnartz: Figure 4 / Element 41 & Column 6 Line 2 – 4, Column 5 Line 63 – 67, Column 8 Line 60 – 67, Column 10 Line 47 – 49: (a) one of the supplemental information (i.e. a medium mark P) on the storage medium with a predetermined value associated a cryptographic function for decryption purpose is qualified as a cryptographic data (b) this medium mark P is recoded on a special wobble of a track with pit-jitter modulation technique is considered as a “property” of the storage medium (Linnartz: Column 5 Line 59 – 60). This supplemental information is obtained from the storage medium as variations in measuring a physical parameter of the storage medium and one way to do this is through the use of a so-called “wobble” (a special modulation pattern on a particular track), as taught by Linnartz (Column 8 Line 60 – 67), which is also consistent with the disclosure of the specification of the instant application (SPEC: Page 1 Line 19 – 22));

reading helper data (W) from the storage medium (Linnartz: Column 6 Line 5: the second piece of the supplemental information (i.e. a watermark W) is simultaneously embedded with the content of the storage medium is considered as helper data (W). Examiner notes Linnartz teaches a storage medium contains two different types of tracks such as wobble track (or a “property” track as recited in the claim) and a regular track that stores the data content, where a medium mark P and a watermark W resides on the wobble track and the regular tracks, respectively).

However, Linnartz does not disclose expressly “granting the access based on an application of a delta-contracting function to the cryptographic data (Y) and the helper data (W)”.

Lotspiech teaches granting the access based on an application of a delta-contracting function to the cryptographic data (Y) and the helper data (W) (Lotspiech : Column 2 Line 26 – 33, Column 4 Line 49 – 57 / Column 7 Line 7 – 13 and Column 3 Line 7 – 9: Lotspiech teaches using typical “error-correcting code” technique to generate sets of encryption key for a player-recorder apparatus with hamming distance between two sets of keys, where the stored (a) compact generating function characterized by Generating Matrix [G] is qualified as a delta-contracting function, (b) the index of the last define set of key is qualified as the cryptographic data (Y), and (c) the redundant bits portion associated with the Generating Matrix [G] used by typical error-correcting code technique related to hamming distance is qualified as the helper data (W) – This is also consistent with the disclosure of the specification of the instant application (SPEC: Page 11 Line 15 – 16: the redundancy bits are taken directly from the helper data), (d) access to content data is granted implicitly with correctly generated decryption key so that the encrypted content can be decrypted correctly and otherwise, decryption would fail and no proper output can be obtained (i.e. access is denied) if the generated decryption key is incorrect (Lotspiech : Column 3 Line 7 – 9)).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Lotspiech within the system of Linnartz because (a) Linnartz teaches storing the supplemental information on the player-

recorder apparatus for generating decryption keys to prevent pirated copies of content

(b) Lotspiech teaches an effective mechanism to store / retrieve the cryptographic security keys with a compact data storage structure of crucial key elements for an authorized player-recorder apparatus (Lotspiech : Column 1 Line 18 – 24, Column 2 Line 10 – 15 and Column 7 Line 7 – 13).

As per claim 2, Linnartz as modified teaches deriving a decryption key (K) for decrypting the content at least from the application of the delta-contracting function (Lotspiech : Column 2 Line 26 – 33, Column 4 Line 49 – 57 / Column 7 Line 7 – 13 and Column 3 Line 7 – 9: Lotspiech teaches using typical “error-correcting code” technique to generate sets of encryption key for a player-recorder apparatus with hamming distance between two sets of keys, where the stored compact generating function characterized by Generating Matrix [G] is qualified as a delta-contracting function).

As per claim 3, Linnartz as modified teaches deriving the decryption key (K) further from data supplied by a playback or recording apparatus (Lotspiech : Column 4 Line 58 – 62: device serial number).

As per claim 7, Linnartz as modified teaches the delta-contracting function involves a combination of a matrix multiplication on the cryptographic data (Y), a linear addition of at least a portion of the helper data (W), a quantization in which the quantization areas are defined by a portion of the helper data (W), and

Art Unit: 2131

error correction decoding (Lotspiech : Column 2 Line 26 – 33, Column 4 Line 49 – 57 / Column 7 Line 7 – 13 and Column 3 Line 7 – 9: Lotspiech teaches using typical “error-correcting code” technique to generate sets of encryption key for a player-recorder apparatus with hamming distance between two sets of keys, where the stored (a) compact generating function characterized by Generating Matrix [G] is qualified as a delta-contracting function, (b) the index of the last define set of key is qualified as the cryptographic data (Y), and (c) the redundant bits portion associated with the Generating Matrix [G] used by typical error-correcting code technique related to hamming distance is qualified as the helper data (W) – This is also consistent with the disclosure of the specification of the instant application (SPEC: Page 11 Line 15 – 16: the redundancy bits are taken directly from the helper data); which is also qualified as a quantization in which the quantization areas related to the hamming distance associated “quantization tolerance”).

6. Claims 4, 5, 6, and 8 – 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Linnartz (U.S. Patent 6,209,092), in view of Lotspiech et al. (U.S. Patent 6,888,944), hereafter referred to as Lotspiech - 944 with “incorporated by reference” of Lotspiech et al. (U.S. Patent 6,118,873), hereafter referred to as Lotspiech - 873.

As per claim 8, Linnartz teaches a device arranged for granting access to content on a storage medium, comprising:

first reading means for obtaining cryptographic data (Y) from a property of the storage medium ((Linnartz: Figure 4 / Element 41 & Column 6 Line 2 – 4 and Column 5 Line 63 – 67, Column 8 Line 60 – 67, Column 10 Line 47 – 49: (a) one of the supplemental information (i.e. a medium mark P) on the storage medium with a predetermined value associated a cryptographic function for decryption purpose is qualified as a cryptographic data (b) this medium mark P is recoded on a special wobble of a track with pit-jitter modulation technique is considered as a “property” of the storage medium (Linnartz: Column 5 Line 59 – 60). This supplemental information is obtained from the storage medium as variations in measuring a physical parameter of the storage medium and one way to do this is through the use of a so-called “wobble” (a special modulation pattern on a particular track), as taught by Linnartz (Column 8 Line 60 – 67), which is also consistent with the disclosure of the specification of the instant application (SPEC: Page 1 Line 19 – 22));

second reading means for reading helper data (W) from the storage medium (Linnartz: Column 6 Line 5: the second piece of the supplemental information (i.e. a watermark W) is simultaneously embedded with the content of the storage medium is considered as helper data (W). Therefore, considering the structure of the reading means, Linnartz teaches a storage medium contains two different types of tracks such as wobble track (or a “property” track as recited in the claim) and a regular track that stores the data content, where a medium mark P and a watermark W resides on the wobble track and the regular tracks, respectively).

However, Linnartz does not disclose expressly access control means for granting the access based on an application of a delta-contracting function to the cryptographic data (Y) and the helper data (W).

Lotspiech - 944 teaches access control means for granting the access based on an application of a delta-contracting function to the cryptographic data (Y) and the helper data (W) (Lotspiech - 944 : Column 2 Line 26 – 33, Column 4 Line 49 – 57 / Column 7 Line 7 – 13 and Column 3 Line 7 – 9: Lotspiech - 944 teaches using typical “error-correcting code” technique to generate sets of encryption key for a player-recorder apparatus with hamming distance between two sets of keys, where the stored (a) compact generating function characterized by Generating Matrix [G] is qualified as a delta-contracting function, (b) the index of the last define set of key is qualified as the cryptographic data (Y), and (c) the redundant bits portion associated with the Generating Matrix [G] used by typical error-correcting code technique related to hamming distance is qualified as the helper data (W) – This is also consistent with the disclosure of the specification of the instant application (SPEC: Page 11 Line 15 – 16: the redundancy bits are taken directly from the helper data), (d) access to content data is granted implicitly with correctly generated decryption key so that the encrypted content can be decrypted correctly and otherwise, decryption would fail and no proper output can be obtained (i.e. access is denied) if the generated decryption key is incorrect (Lotspiech - 944 : Column 3 Line 7 – 9)). (e) Additionally, Examiner notes the output of the delta-contracting function, as taught by Lotspiech – 944, that generates a set of device keys are used to decrypt the encrypted session secret

Art Unit: 2131

numbers and all of the decrypted session secret numbers are then hashed to produce a content session key (Lotspiech – 873: Column 6 Line 30 – 37 and Column 2 Line 10 – 14) and Linnartz also teaches hashing (XOR) the seeds (i.e. secret numbers) coupled with a “one-way function” operation for a predetermined number of times (or cycles) in order to generate a control pattern to be validated against an embedded watermark (i.e. the generated content session key is equivalent to the control pattern to be validated against the embedded watermark (Linnartz: Column 8 Line 40 – 41) where the watermark / control pattern is embedded in the storage medium (Linnartz: Column 6 Line 5 – 6) – This is also consistent with the disclosure of the specification of the instant application that compares the result against the control value (V) stored on the storage medium).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Lotspiech - 944 within the system of Linnartz because (a) Linnartz teaches storing the supplemental information on the player-recorder apparatus for generating decryption keys to prevent pirated copies of content (b) Lotspiech - 944 teaches an effective mechanism to store / retrieve the cryptographic security keys by using a compact data storage structure of crucial key elements for an authorized player-recorder apparatus (Lotspiech - 944 : Column 1 Line 18 – 24, Column 2 Line 10 – 15 and Column 7 Line 7 – 13).

As per claim 4, Linnartz as modified teaches the access is granted if the output of the delta-contracting function corresponds to a control value (V) recorded on the

Art Unit: 2131

storage medium (Lotspiech - 944: Column 4 Line 49 – 57 / Column 7 Line 7 – 13; Lotspiech – 873: Column 6 Line 30 – 37 and Column 2 Line 10 – 14; Linnartz: Column 8 Line 26 – 40: (a) The output of the delta-contracting function, as taught by Lotspiech – 944, that generates a set of device keys are used to decrypt the encrypted session secret numbers and all of the decrypted session secret numbers are then hashed to produce a content session key, as taught by Lotspiech – 873, and (b) Linnartz also teaches hashing (XOR) the seeds (i.e. secret numbers) coupled with a “one-way function” operation for a predetermined number of times (or cycles) in order to generate a control pattern to be validated against an embedded watermark (i.e. the generated content session key is equivalent to the control pattern to be validated against the embedded watermark (Linnartz: Column 8 Line 40 – 41), where the watermark / control pattern is embedded in the storage medium (Linnartz: Column 6 Line 5 – 6)).

As per claim 5, Linnartz as modified teaches applying a cryptographic function to the output of the delta-contracting function and comparing the output of the cryptographic function to the control value (V) (Lotspiech - 944: Column 4 Line 49 – 57 / Column 7 Line 7 – 13; Lotspiech – 873: Column 6 Line 30 – 37 and Column 2 Line 10 – 14; Linnartz: Column 8 Line 26 – 40: (a) The output of the delta-contracting function, as taught by Lotspiech – 944, that generates a set of device keys are used to decrypt the encrypted session secret numbers and all of the decrypted session secret numbers are then hashed to produce a content session key, as taught by Lotspiech – 873, and

(b) Linnartz also teaches hashing (XOR) the seeds (i.e. secret numbers) coupled with a “one-way function” operation for a predetermined number of times (or cycles) in order to generate a control pattern to be validated against an embedded watermark (i.e. the generated content session key is equivalent to the control pattern to be validated against the embedded watermark (Linnartz: Column 8 Line 40 – 41) where the watermark / control pattern is embedded in the storage medium (Linnartz: Column 6 Line 5 – 6)).

As per claim 6, Linnartz as modified teaches the cryptographic function is a one-way hash function (Lotspiech – 873: Column 6 Line 36; Linnartz: Column 8 Line 26 – 40: (a) Lotspiech – 873 teaches using hash function to hash all of the decrypted session secret number to produce a content session key – Examiner notes a hash function with “one-way” operation such as MD5 is a well-known technique indicated herein as Applicant Admitted Prior-art (SPEC: Page 8 Line 15 – 16) that is desirable because there is no practical way to calculate a particular data input that will result in a desired hash value, so it is also very difficult to forge, (b) Linnartz also teaches hashing (XOR) the seeds (i.e. secret numbers) coupled with a “one-way function” operation for a predetermined number of times (or cycles) in order to generate a control pattern to be validated against an embedded watermark).

As per claim 9, Linnartz as modified teaches effecting the playback and/or recording if access is granted by the device (Lotspiech - 944 : Column 3 Line 7 – 9: to playback, the encrypted content must be decrypted correctly).

As per claim 10, Linnartz as modified teaches a computer program product arranged to cause a processor to execute the method of claim (Lotspiech - 944 : Column 2 Line 19 – 22).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2131

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Longbit Chai/

Longbit Chai Ph.D.

Primary Examiner, Art Unit 2131

4/20/2008